

REMARKS

Claims 1 - 21, 23, and 26 - 31 are pending. Claims 22, 24, and 25 have been cancelled. Claims 30 and 31 have been added. Claims 1 - 21, 23, and 26 - 29 have been amended. No new matter has been introduced. Reexamination and reconsideration of the present application are respectfully requested.

In the Office Action dated April 5, 2005, the Examiner objected to the drawings because a number of reference characters were not mentioned in the description. The specification has been amended to include the corresponding reference numbers. The applicants respectfully submit that the objection to the drawings should be withdrawn.

In the Office Action dated April 5, 2005, the Examiner objected to claim 4 due to informalities and also under 35 U.S.C. § 112, second paragraph. Claim 4 has been amended in order to address these concerns and to further define the invention.

In the Office Action dated April 5, 2005, the Examiner rejected claims 1 - 3, 6, 7, 10, 11, 14, 15, and 18 under 35 U.S.C. § 102(b) as being anticipated by Schneier, Applied Cryptography. The Examiner rejected claims 4, 5, 8, 9, 12, 13, 16, 17, and 19 - 29 under 35 U.S.C. § 103(a) as being unpatenable over Schneier, Applied Cryptography. These rejections, in so far as applicable to the presently pending claims, are respectfully traversed.

Claim 1, as amended, distinguishes over the Schneier reference. Claim 1, as amended, recites:

A method, comprising:
sending, from a sender to a receiver, data through a data channel,
the data including a key and a nonce;
receiving, at the receiver, the data;
**establishing a visual physical channel between the sender and
the receiver, the sender and receiver being visible to each other; and**

verifying, between the receiver and the sender via the visual physical channel, that the data is from the sender by having the receiver respond by sending a repeating nonce to the sender, wherein the repeating nonce is an action requested in the nonce.

The Schneier reference does not disclose, teach, or suggest the method of claim 1, as amended. The Schneier reference discloses authentication protocols using timestamps where a two-way protocol includes a message from Alice and a reply from Bob. For example, Alice can construct a random number, and constructs a message including a timestamp, a receiver's identity, and an arbitrary piece of data. Alice also sends her digital certificate and a private key to Bob. Bob verifies the certificate and obtains Alice's public key and utilizes the public key to decrypt the private key. Bob then checks his identity in the message for accuracy and checks the message is current. (*Schneier, page 576*). There is no discussion of **establishing a visual physical channel, where the sender and receiver are visible to each other**, as is recited in claim 1, as amended.

Further, the Schneier reference does not disclose the receiving of a repeating nonce, **wherein the repeating nonce is an action requested in the nonce**. The Schneier reference discloses that Bob responds to Alice's message by generating a message of his own, wherein the message includes Bob's timestamp, Alice's identity, and arbitrary data. The data may be encrypted with Alice's public key. (*Schneier, page 577*). However, the Schneier reference is not disclosing that **a generated repeating nonce is an action requested in the nonce**, as is recited in claim 1, as amended. There is no correlation between the arbitrary data in Alice's message and Bob's responding message and no action being performed as requested in the nonce. Accordingly, claim 1, as amended, distinguishes over the Schneier reference.

Claim 14, as amended, recites limitations similar to claim 1, as amended.

Accordingly, applicants respectfully submit that claim 14 distinguishes over the Schneier reference for reasons similar to those discussed above in regard to claim 1.

Claims 2 - 5 and 15 - 17 depend, indirectly or directly, on claims 1 and 14, respectively. Accordingly, applicants respectfully submit that claims 2 - 5 and 15 - 17 distinguish over the Schneier reference for the same reasons as those discussed above in regard to claim 1.

Claims 2 and 3 further distinguish over the Schneier reference. Claim 2, as amended, recites:

The method according to claim 1, **wherein the repeating nonce is a hand gesture.**

Claim 3, as amended, recites:

The method according to claim 1, **wherein the repeating nonce is an audio signal.**

The Schneier reference does not disclose, teach or suggest the method of claims 2 and 3. The Schneier reference never discloses the user of a hand gesture and/or an audio signal, as are recited in claims 2 and 3, in order to verify that data has been sent. Accordingly, applicants respectfully submit that claims 2 and 3 distinguish over the Schneier reference.

Claim 6 distinguishes over the cited reference. Claim 6, as amended, recites:

A method for a sender, comprising:
establishing a physical channel with a receiver;
sending, from the sender to the receiver, data through a data channel, the data including a key and a nonce; and
verifying, between the sender and the receiver via the physical channel, that the receiver receives the data from the sender by receiving a responding nonce from the receiver, **the responding nonce being a response to an action requested by the nonce.**

The Schneier reference does not disclose, teach, or suggest the method of claim 6, as amended. The Schneier reference discloses only that the originating sender, e.g., Alice, receives a message from Bob including Bob's timestamp, the identity of Alice, and arbitrary data. (Schneier, page 576 and 577). There is no disclosure that the responding nonce, received from the sender is a response to an action requested by the nonce. Accordingly, applicants respectfully submit that claim 6 distinguishes over the Schneier reference.

Independent claims 10, 18, 21, 26, and 28, all as amended, recite limitations similar to claim 6, as amended. Accordingly, applicants respectfully submit that claims 10, 18, 21, 26, and 28 distinguish over the Schneier reference for reasons similar to those discussed above in regard to claim 6, as amended.

Claims 7 - 9, 12 - 13, 19, 20, 24, 27, 29, 30, and 31 depend, directly or indirectly on claims 6, 10, 18, 21, 26, and 29. Accordingly, applicants respectfully submit that claims 7 - 9, 12 - 13, 19, 20, 24, 27, 30, and 31 distinguish over the Schneier reference for the same reasons as those discussed above in regard to claim 6.

Claims 7 and 8 further distinguish over Schneier reference. Claim 7, as amended, recites:

The method according to claim 6, wherein the **responding nonce is one of a sum of two numbers transmitted as the nonce; a multiplication of the two numbers, or a division of the two numbers.**

Claim 8, as amended, recites:

The method according to claim 6, wherein the **responding nonce is an audio signal including a phrase spoken in a language requested in the nonce.**

There is no disclosure in the Schneier reference that the responding nonce (or responding message) is the sum of two numbers transmitted previously as the nonce, the multiplication of the two numbers or a division of the two numbers. Nor does the Schneier reference disclose that the responding nonce is an audio signal including a spoken phrase. Accordingly, applicants respectfully submit that claims 7 and 8 distinguish over the Schneier reference.

Claims 12 - 13, 19 - 20, 23, 27, 29, 30, and 31 recite limitations similar to claims 7 and 8. Accordingly, applicants respectfully submit that claims 12 - 13, 19 - 20, 23, 27 - 29, 30, and 31 distinguish over the Schneier reference for reasons similar to those discussed above in regard to claims 7 and 8.

///

///

///

///

///

///

///

///

///

///

///

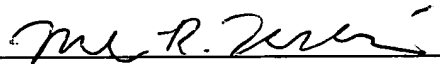
///

Applicants believe that the foregoing amendments place the application in condition for allowance, and a favorable action is respectfully requested. If for any reason the Examiner finds the application other than in condition for allowance, the Examiner is requested to call either of the undersigned attorneys at the Los Angeles telephone number (213) 488-7400 to discuss the steps necessary for placing the application in condition for allowance should the Examiner believe that such a telephone conference would advance prosecution of the application.


Respectfully submitted,

PILLSBURY WINTHROP LLP

Date: July 5, 2005

By: 
Mark R. Kendrick
Registration No. 48,468
Attorney for Applicant(s)

Date: July 5, 2005

By: 
Roger R. Wise
Registration No. 31,204
Attorney for Applicant(s)

725 South Figueroa Street, Suite 2800
Los Angeles, CA 90017-5406
Telephone: (213) 488-7100
Facsimile: (213) 629-1033